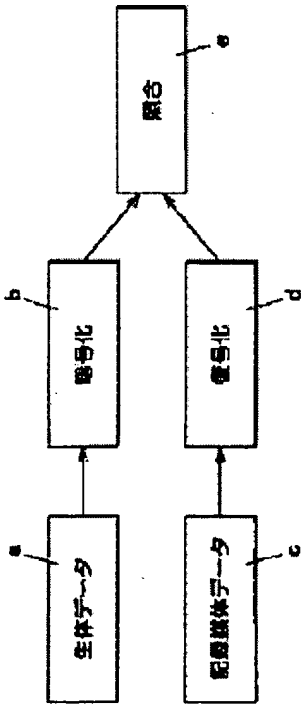
F1

USER AUTHENTICATION METHOD AND SYSTEM USING BIOLOGICAL INFORMATION AND DATA RECORDING MEDIUM, AND PROGRAM RECORDING MEDIUM

Publication number: JP2002132731
Publication date: 2002-05-10
Inventor: ITAKURA HIROKAZU; OKADA KENICHI; UENO KEIJI
Applicant: HITACHI SYSTEMS & SERVICES LTD
Classification:
- international: ***G06F15/00; H04L9/32;*** **G06F15/00; H04L9/32;** (IPC1-7): G06F15/00; G06F17/60; H04L9/32
- european:
Application number: JP20000322394 20001023
Priority number(s): JP20000322394 20001023

Abstract of **JP2002132731**

PROBLEM TO BE SOLVED: To make a user authentication system high in security level. SOLUTION: In order to authenticate a user, biological data (a) are acquired from the user and by enciphering (b) these data, collation data on one side are generated. On the other hand, parallel with the acquisition of the biological data (a), previously enciphered data (c) are read out of a data recording medium, that the user has, and by deciphering (d) these data, collation data on the other side are generated. It is collated (e) whether these collation data are equal or not. Thus when both the data are equal to each other, the user is authenticated as a authorized user.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2002－132731
（P2002－132731A）
(43)公開日　平成14年５月10日(2002.5.10)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'（参考）
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｆ	５Ｂ０８５
			３３０Ｅ	５Ｊ１０４
17/60	５１２	17/60	５１２	
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７３Ｃ	
			６７３Ｄ	

審査請求　未請求　請求項の数10　ＯＬ　（全 12 頁）　最終頁に続く

(21)出願番号　特願2000－322394(P2000－322394)

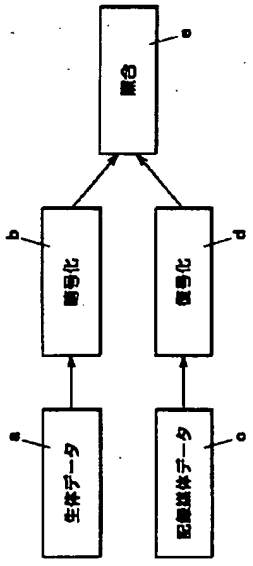
(22)出願日　平成12年10月23日(2000.10.23)

(71)出願人　391002409
株式会社　日立システムアンドサービス
東京都大田区大森北３丁目２番16号
(72)発明者　板倉　博和
大阪府大阪市中央区内本町２丁目４番16号
株式会社日立システムアンドサービス内
(72)発明者　岡田　健一
大阪府大阪市中央区内本町２丁目４番16号
株式会社日立システムアンドサービス内
(74)代理人　100092956
弁理士　古谷　栄男　（外２名）

最終頁に続く

(54)【発明の名称】　生体情報とデータ記録媒体を用いたユーザ認証方法、認証装置およびプログラム記録媒体

(57)【要約】
【目的】利用者の認証システムにおいて、セキュリティーレベルの高い認証システムを提供する。
【構成】利用者の認証を行うために、利用者から生体データaを取得し、これを暗号化bすることで片方の照合データを生成する。一方、生体データaを取得するのと並行して、利用者が有するデータ記録媒体から予め暗号化されたデータcを読み出し、これを復号化dすることで、もう片方の照合データを生成する。これらの照合データが同一のものであるか否かを照合eする。その結果、両データが同一である場合には、正当な利用者であるとの認証がなされる。



【特許請求の範囲】
【請求項１】利用者の生体情報を少なくとも一回暗号化した第１の暗号化生体データを予め記録したデータ記録媒体から、当該第１の暗号化生体データを読み出す読出手段と、
利用時において、利用者からその生体情報を取得する生体情報取得手段と、
生体情報取得手段からの生体情報を少なくとも一回暗号化して第２の暗号化生体データを得るとともに、読出手段によって読み出した第１の暗号化生体データに基づいて得た第３の暗号化生体データと、第２の暗号化生体データとを比較照合する照合手段と、
を備えたことを特徴とする認証装置。
【請求項２】利用者の生体情報を少なくとも一回暗号化した第１の暗号化生体データを予め記録したデータ記録媒体から、当該第１の暗号化生体データを読み出し、
利用時において、利用者からその生体情報を取得し、
当該利用者から取得した生体情報を少なくとも一回暗号化して第２の暗号化生体データを得るとともに、データ記録媒体から読み出した第１の暗号化生体データに基づいて得た第３の暗号化生体データと、第２の暗号化生体データとを比較照合する処理を認証装置に実行させるためのプログラム、
を記録したことを特徴とするプログラム記録媒体。
【請求項３】請求項１の認証装置又は請求項２のプログラム記録媒体において、
前記第３の暗号化生体データとして、前記第１の暗号化生体データをそのまま用いることを特徴とするもの。
【請求項４】請求項１の認証装置又は請求項２のプログラム記録媒体において、
前記第１の暗号化生体データは、利用者の生体情報を２重に暗号化しており、
前記第３の暗号化生体データは、前記第１の暗号化生体データを１回復号化したものであることを特徴とするもの。
【請求項５】請求項４の認証装置又はプログラム記録媒体において、
前記第１の暗号化生成データは、利用者の生体情報を第１の非対称鍵で二重に暗号化しており、
前記第３の暗号化生成データは、当該第１の暗号化生成データを第２の非対称鍵で１回復号化したものであることを特徴とするもの。
【請求項６】請求項５の認証装置又はプログラム記録媒体において、
前記データ記録媒体は、さらに、第１の非対称鍵データおよび第２の非対称鍵を共通鍵を用いて少なくとも１回暗号化した暗号化非対称鍵データを記録しており、
前記第３の暗号化生成データは、認証時に利用者から取得したデータに基づいて生成した前記共通鍵を用いて当該暗号化非対称鍵データを１回復号化して生成する第２の非対称鍵を用いて、前記第１の暗号化生成データを復号化することにより得ることを特徴とするもの。
【請求項７】利用者の生体情報を記録したデータ記録媒体であって、
少なくとも生体情報を２重暗号化して記録したことを特徴とするもの。
【請求項８】利用者の生体情報を記録したデータ記録媒体であって、
少なくとも生体情報を第１の非対称鍵で２重暗号化したデータ、第１の非対称鍵データ、第２の非対称鍵を少なくとも１回暗号化したデータを記録したことを特徴とするもの。
【請求項９】請求項７または請求項８のデータ記録媒体において、
前記データ記録媒体は、電子透かしを組み込んだ識別子を備えたことを特徴とするもの。
【請求項１０】利用者の生体情報を少なくとも一回暗号化した第１の暗号化生体データをデータ記録媒体に予め記録しておき、
利用時においては、前記データ記録媒体から第１の暗号化生成データを読み出すとともに、利用者からその生体情報を取得し、
当該利用者から取得した生体情報を少なくとも一回暗号化して第２の暗号化生体データを得るとともに、データ記録媒体から読み出した第１の暗号化生体データに基づいて得た第３の暗号化生体データと、第２の暗号化生体データとを比較照合すること、
を特徴とする利用者の認証方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】この発明は、システムを利用する利用者の認証技術に関し、特に、そのセキュリティーレベルの向上に関する。
【０００２】
【従来の技術】近年、コンピュータシステムの発展により、産業の活性化や社会の利便性の拡大が進む反面、データ侵害やプライバシー侵害などのコンピュータ犯罪も増加するなど、その弊害も問題視されつつある。このような、犯罪行為から保護すべき対象となるべき情報は、企業利益に関わるもの、銀行業務など金融、決済に関わるもの、個人の情報に関わるものなど多様化してきている。
【０００３】このような保護すべき情報を悪意の第三者による犯罪行為から守るための技術は、一般に、情報セキュリティー技術と呼ばれる。情報セキュリティー技術は、第三者の不正行為の形態によって、認証技術、アクセス制御技術、隔離技術、監視技術などに分類することができる。この発明は、特に認証技術に関するものである。
【０００４】認証技術は、利用者が正当であるか否かを

確認すること（利用者認証）を目的とする情報セキュリティー技術である。利用者認証には、パスワードによる認証が用いられることが多い。しかし、パスワードのみを用いた認証では、利用者の記憶に依存するため、あまり多くの文字のパスワードを用いることができないという制限がある。このため、これとは別に利用者個人の属性情報を用いた認証や、利用者の所有物による認証が用いられている。

【０００５】個人の属性情報を用いた認証では、指紋、声紋、筆跡、網膜の眼紋を属性情報とし、これを比較照合する方式が考えられている。また、所有物による認証では、印鑑の印影の比較照合があるが、最近ではICカードが多く用いられている。

【０００６】なお、指紋を用いた個人認証方法は、その他の属性情報を用いた認証方法よりも確実な認証手段であり、世界中の国々で警察の分野を中心に利用されている。指紋の特徴は、隆線の指全体における流れのパターンによって表され、判別方法としては、尖点、デルタ点、渦点などの特徴点を検出し、その数と位置関係によって分類する方法などがある。

【０００７】また、さらに個人の属性情報と所有物による認証を組み合わせることでセキュリティレベルを高めた方式も存在する。例えば、指紋データを認証時に入力し、ICカードに利用者の当該指紋データを記録しておき両データを比較照合する認証方式が該当し、実際にはコンピュータ室などへの入退管理用として利用されている。

【発明が解決しようとする課題】しかし、このような従来の生体情報（個人の属性情報）とデータ記録媒体（個人の所有物）の組み合わせによるユーザ認証方式では、データ記録媒体から読み出した生体情報に基づくデータと、認証時に認証装置に入力した生体情報に基づくデータとを単に比較することにより利用者の認証が行われていた。

【０００８】このため、データ記録媒体や認証装置に記録された認証データの解読や、これによるデータ記録媒体の捏造、認証データの悪用などが比較的容易に実施される危険性があった。

【０００９】また、ネットワーク上のサーバ側にもユーザ認証情報を記録しておくような場合には、認証情報データの改竄、成り済ましによるシステム破壊などの驚異にもさらされる可能性があった。

【００１０】

【課題を解決するための手段および発明の効果】（１）この発明の認証装置は、利用者の生体情報を少なくとも一回暗号化した第１の暗号化生体データを予め記録したデータ記録媒体から、当該第１の暗号化生体データを読み出す読出手段と、利用時において、利用者からその生体情報を取得する生体情報取得手段と、生体情報取得手段からの生体情報を少なくとも一回暗号化して第２の暗号化生体データを得るとともに、読出手段によって読み出した第１の暗号化生体データに基づいて得た第３の暗号化生体データと、第２の暗号化生体データとを比較照合する照合手段と、を備えたことを特徴とする。

【００１１】したがって、データ記録媒体に生体情報を暗号化して登録することにより、元の生体情報の解読を困難にすることができる。このため、第三者がデータ記録媒体を捏造することを防止することができる。

【００１２】また、暗号化した状態で比較照合するため第三者が認証のためのデータを特定し、盗用することが困難となる。

【００１３】さらに、利用者の認証を読出装置と生体情報取得手段の組み合わせにより認証装置のみで実行することができる。このため、不正利用者によるサーバへのアクセスやネットワークへの侵入を認証装置でのチェックにより拒否し、システムへの不正侵入を未然に防止することができる。このため、セキュリティーレベルの高いシステムを構築することができる。

【００１４】（２）この発明のプログラム記録媒体は、利用者の生体情報を少なくとも一回暗号化した第１の暗号化生体データを予め記録したデータ記録媒体から、当該第１の暗号化生体データを読み出し、利用時において、利用者からその生体情報を取得し、当該利用者から取得した生体情報を少なくとも一回暗号化して第２の暗号化生体データを得るとともに、データ記録媒体から読み出した第１の暗号化生体データに基づいて得た第３の暗号化生体データと、第２の暗号化生体データとを比較照合する処理を認証装置に実行させるためのプログラム、を記録したことを特徴とする。

【００１５】したがって、データ記録媒体に生体情報を暗号化して登録することにより、元の生体情報の解読を困難にすることができる。このため、第三者がデータ記録媒体を捏造することを防止することができる。

【００１６】また、暗号化した状態で比較照合するため第三者が認証のためのデータを特定し、盗用することが困難となる。

【００１７】さらに、利用者の認証を読出装置と生体情報取得手段の組み合わせにより認証装置のみで実行することができる。このため、不正利用者によるサーバへのアクセスやネットワークへの侵入を認証装置でのチェックにより拒否し、システムへの不正侵入を未然に防止することができ、セキュリティーレベルの高いシステムを構築することができる。

【００１８】（３）この発明は、前記第３の暗号化生体データとして、前記第１の暗号化生体データをそのまま用いることを特徴とする。

【００１９】したがって、認証時に必要な暗号化等の処理を可能な限り簡素にしつつ、セキュリティーレベルの高いシステムを構築することができる。

【００２０】（４）この発明は、前記第１の暗号化生体

データは、利用者の生体情報を２重に暗号化しており、前記第３の暗号化生体データは、前記第１の暗号化生体データを１回復号化したものであることを特徴とする。

【００２１】したがって、認証時に常に暗号化および復号化を行うことで照合の際のアルゴリズムが複雑となる。このため、セキュリティーレベルの高いシステムを構築することができる。

【００２２】（５）この発明は、前記第１の暗号化生成データは、利用者の生体情報を非対称鍵で二重に暗号化しており、前記第３の暗号化生成データは、当該第１の暗号化生成データを非対称鍵で１回復号化したものであることを特徴とする。

【００２３】したがって、認証時に常に非対称鍵により暗号化および復号化を行うことで照合の際のアルゴリズムが複雑となる。このため、セキュリティーレベルの高いシステムを構築することができる。

【００２４】（６）この発明は、前記データ記録媒体は、さらに、第１の非対称鍵データおよび第２の非対称鍵を共通鍵を用いて少なくとも１回暗号化した暗号化非対称鍵データを記録しており、前記第３の暗号化生成データは、認証時に利用者から取得したデータに基づいて生成した前記共通鍵を用いて当該暗号化非対称鍵データを１回復号化して生成する第２の非対称鍵を用いて、前記第１の暗号化生成データを復号化することにより得ることを特徴とする。

【００２５】したがって、認証時に常に非対称鍵により暗号化および復号化を行うことで照合の際のアルゴリズムが複雑となる。このため、セキュリティーレベルの高いシステムを構築することができる。

【００２６】（７）この発明のデータ記録媒体は、利用者の生体情報を記録したデータ記録媒体であって、少なくとも生体情報を２重暗号化して記録したことを特徴とする。

【００２７】したがって、利用者の認証を読出装置と生体情報取得手段の組み合わせにより認証装置のみで実行することができる。このため、不正利用者によるサーバへのアクセスやネットワークへの侵入を認証装置でのチェックにより拒否し、システムへの不正侵入を未然に防止することができ、セキュリティーレベルの高いシステムを構築することができる。

【００２８】（８）この発明は、利用者の生体情報を記録したデータ記録媒体であって、少なくとも生体情報を第１の非対称鍵で２重暗号化したデータ、第１の非対称鍵データ、第２の非対称鍵を少なくとも１回暗号化したデータを記録したことを特徴とする。

【００２９】したがって、利用者の認証を読出装置と生体情報取得手段の組み合わせにより認証装置のみで実行することができる。このため、不正利用者によるサーバへのアクセスやネットワークへの侵入を認証装置でのチェックにより拒否し、システムへの不正侵入を未然に防止することができ、セキュリティーレベルの高いシステムを構築することができる。

【００３０】（９）この発明は、利用者の生体情報を記録したデータ記録媒体であって、前記データ記録媒体は、電子透かしを組み込んだ識別子を備えたことを特徴とする。

【００３１】したがって、データ記録媒体の真贋を容易に判断することができ、媒体の捏造防止を強化することができる。

【００３２】（１０）この発明の利用者の認証方法は、利用者の生体情報を少なくとも一回暗号化した第１の暗号化生体データをデータ記録媒体に予め記録しておき、利用時においては、前記データ記録媒体から第１の暗号化生成データを読み出すとともに、利用者からその生体情報を取得し、当該利用者から取得した生体情報を少なくとも一回暗号化して第２の暗号化生体データを得るとともに、データ記録媒体から読み出した第１の暗号化生体データに基づいて得た第３の暗号化生体データと、第２の暗号化生体データとを比較照合すること、を特徴とする。

【００３３】したがって、データ記録媒体に生体情報を暗号化して登録することにより、元の生体情報の解読を困難にすることができる。このため、第三者がデータ記録媒体を捏造することを防止することができる。

【００３４】また、暗号化した状態で比較照合するため、第三者が認証のためのデータを特定し、盗用することが困難となる。

【００３５】さらに、利用者の認証を読出装置と生体情報取得手段の組み合わせにより認証装置のみで実行することができる。このため、不正利用者によるサーバへのアクセスやネットワークへの侵入を認証装置でのチェックにより拒否し、システムへの不正侵入を未然に防止することができ、セキュリティーレベルの高いシステムを構築することができる。

【００３６】

【発明の実施の形態】[発明の概要について]まず、図１を用いて、この発明の概要について説明する。

【００３７】この発明は、データ記録媒体を用いてユーザ認証を行うものである。したがって、ユーザ認証を受ける利用者には、認証に用いられるデータ記録媒体が予め配布されている。このデータ記録媒体には、例えば、指紋などの生体データを２重暗号化したデータ（記録媒体データｃ）が記録されている。

【００３８】以下に、このデータ記録媒体を有する利用者がユーザ認証を受ける際に、認証装置において行われる処理について説明する。

【００３９】まず、図１に示すように、生体情報取得手段は、認証時に利用者から生体データａを取得し、これを１重暗号化ｂする処理を行う。これにより、一方の照合データ（第２の暗号化生体データ）が生成される。

【００４０】その一方で、読出手段は、データ記録媒体から前述した２重暗号化された記録媒体データ（第１の暗号化生体データ）cを読み出し、さらに、このデータを復号化dし、１重暗号化したデータに戻す処理を行う。これにより、もう一方の照合データ（第３の暗号化生体データ）が生成される。

【００４１】照合手段は、これらの一重暗号化された照合データ（第２および第３の暗号化生体データ）が同じであるか否かを照合eする処理を行う。その結果、両データが同一である場合には、正当な利用者であると認証し、認証装置のセキュリティー保護状態が解除される。

【００４２】このように、照合を暗号化した状態で行うことにより、第三者によるデータの特定、盗用が困難となり、セキュリティーレベルを高めることが可能となる。

【００４３】以下に、生体情報として利用者の指紋を用い、データ記録媒体としてICカードを用いた場合の実施形態について説明する。

【００４４】[実施形態の概要について]図2は、この発明の実施形態の概念図である。

【００４５】ユーザ認証を受ける利用者には、認証に用いられるICカードが予め配布されている。なお、このICカードには、指紋データｆを公開鍵Ｐ（第１の非対称鍵）によって二重の暗号化したデータＰ[P[f]]、公開鍵データＰ、パスワードWに基づいて生成した共通鍵Wcによって秘密鍵Ｓ（第２の非対称鍵）を暗号化したデータWc[S]が、予め記録されている。なお、Ｐ[f]は、データｆをデータＰを用いて暗号化処理したことを意味する。

【００４６】以下に、このICカードを有する利用者が、認証を受ける際に認証装置において行われる処理について説明する。

【００４７】図2に示すように、生体情報取得手段は、まず、指紋から指紋データｆ’を採取する。さらに、この指紋データｆ’は、ICカードより読み出した公開鍵Ｐによって暗号化処理され、データＰ[f’]になる。この一重暗号化処理したデータＰ[f’]が、比較照合される一方の照合データとなる。

【００４８】一方で、認証を受ける利用者は、パスワードWを入力する。認証装置では、このパスワードWに基づいて生成した共通鍵Wcによって、図２に示すように、ICカードより読み出したデータWc[S]（共通鍵Wcによって秘密鍵Ｓを予め暗号化したデータ）が復号化処理され、秘密鍵Ｓが生成される。

【００４９】さらに、この生成された秘密鍵Ｓによって、ICカードより読み出したデータＰ[P[f]]を復号化処理しＰ[f]とする。この一重暗号化したデータＰ[f’]が、比較照合される、もう一方の照合データとなる。

【００５０】照合手段は、上記処理により生成された照合データP[f’](指紋から採取したデータに基づいて生成された一重暗号化データ)と照合データP[f](データ記録媒体から読み出したデータに基づいて生成された一重暗号化データ)を照合する。その結果、両データが同一であれば利用者として認証し、認証装置におけるセキュリティー保護状態は解除される。一方、両データが同一でなければ利用者として認証されないため、認証装置のセキュリティー保護状態は解除されないことになる。

【００５１】[システム構成]以下に、図３および図４を用いて、この発明の一実施形態のシステム構成について説明する。なお、図３は、この発明をネットワーク利用者の認証に用いた場合のシステム構成を示す。図４は、認証装置の構成を示す図である。

【００５２】図３に示すように、この発明を実施するためのシステムは、ネットワーク３を介してサーバ１と複数の認証装置であるクライアントＰＣ５が相互に通信可能なように接続されたものとなっている。

【００５３】サーバ１には、盗用などの犯罪行為から保護すべきデータが記録されている。例えば、企業利益に関わるもの、銀行業務など金融、決済に関わるもの、個人の情報に関わるものなどである。

【００５４】ネットワーク３には、LAN、インターネットなどの通信手段が用いられる。

【００５５】認証装置であるクライアントＰＣ５は、図４に示すように、CPU２０、メモリ２２、ディスプレイ２４、ハードディスク２６、キーボード／マウス２８、読出手段であるICカードリーダ３０、生体情報取得手段である指紋データリーダ３４を備える。

【００５６】クライアントＰＣ５のハードディスク２６には、マイクロソフト社のウインドウズなどのオペレーションシステム（OS）がインストールされている。また、照合手段である照合ソフトも、ハードディスク２６にインストールされている。

【００５７】この照合ソフトは、認証データを比較照合することで正当な利用者であるか否かを判断する処理を行う機能だけでなく、非対称鍵方式、共通鍵方式を用いたデータの暗号化および復号化処理を行う機能を備える。CPU２０は、この暗号化および復号化処理などに必要な演算を行う。

【００５８】なお、非対称鍵方式とは、対になる2つの鍵を使ってデータの暗号化・復号化を行なう暗号方式のことであり、公開鍵方式とも呼ばれるものである。片方は他人に広く公開するため公開鍵と呼ばれ、もう片方は本人だけがわかるように厳重に管理されるため秘密鍵と呼ばれる。秘密鍵で暗号化されたデータは対応する公開鍵でしか復号できず、公開鍵で暗号化されたデータは対応する秘密鍵でしか復号できない。このため鍵を安全な経路で輸送する必要がなく、共通鍵暗号方式に比べて鍵の管理が楽で安全性が高い。具体的な暗号化方式としては、巨大な整数の素因数分解の困難さを利用したRSA方式などがある。

【００５９】これに対して、共通鍵方式とは、暗号化と

復号化に同じ鍵を用いる暗号方式をいう。このため、暗号文を送受信する前に、あらかじめ安全な経路を使って秘密の鍵を共有する必要がある。代表的な共通鍵暗号としては、DES、FEAL、MISTY、IDEA、などの方式がある。読出手段であるICカードリーダ３０は、ICカード３２のICチップなどに記録された認証のためのデータ（認証データ）を読み出す機能を備える。

【００６０】データ記録媒体であるICカード３２には、認証データが記録できるICチップが組み込まれている。このICチップには、利用者の生体情報に基づくデータなどが予め記録されている。

【００６１】また、このICカード３２は、偽造防止のために電子透かしを組み込んだホログラムなどの識別子を備える。電子透かしとは、画像や音声を損なわない範囲で直接画像や音声データに別の情報を書き込む技術であり、ここではICカード３２の真贋の判断に利用される。

【００６２】生体情報取得手段である指紋データリーダ３４は、クライアントＰＣ５の利用時において利用者からその指紋情報を取得する機能を備える。具体的な、指紋データリーダ３４としては、 ソニーの「Sony Finger print Identification UnitFIU-700」、富士通の「Fing sensor FS-200P」などを用いることができる。

【００６３】［ICカードに認証データを記録する処理］前述したように、この実施形態においては認証時にICカードがデータ記録媒体として用いられる。したがって、ユーザ認証を行うためには、ICカードを作成し、ユーザ認証を受ける利用者に対して予め配布しておく必要がある。

【００６４】以下に、図５および図６を用いて、この認証に用いるデータを記録するICカードを作成する手順について説明する。なお、図５は、ICカードを生成するICカード生成装置の構成を示した図である。図６は、認証に用いるデータをICカードに認証データを記録するまでの処理を示すフローチャートである。

【００６５】図５に示すように、ICカード生成装置は、CPU２０、メモリ２２、ディスプレイ２４、ハードディスク２６、キーボード／マウス２８、ICカードライタ３１、生体情報取得手段である指紋データリーダ３４を備える。

【００６６】ICカードライタ３１は、ICカード３２の記憶部に、認証データを書き込む機能を備える。また、ICカード生成装置のハードディスク２６には、データを暗号化および復号化処理する暗号ソフトがインストールされている。CPU２０は、これらの暗号化および復号化などの処理に必要な演算を行う。

【００６７】まず、認証を受けようとする利用者は、ICカード生成装置の指紋データリーダ３４に指を触れる。これによって、指紋データリーダ３４は、図６に示すように、指紋の読み込みを開始する（ステップＳ１０１）。さらに、指紋データリーダ３４は、指紋の特徴を抽出して、指紋データｆを生成する（ステップＳ１０３）。ここでは、指紋というアナログデータからデジタルデータを生成する処理が行われる。

【００６８】この指紋データｆを取得するための処理は、一定のアルゴリズムによって行われる。例えば、一般的に隆線の開始点、分岐点などのマイニューシャ（minutiae）の特徴からデータを取得することによりおこなわれる。なお、マイニューシャは、一指に平均１００個あり、二つの指紋の間で１２個以上のマイニューシャが一致すれば、同一人同一指の指紋と断定することができるとされている。従って、ここで取得される指紋データが、１２個以上のマイニューシャの特徴に基づくデータであれば、利用者の認証において十分な認識率を得ることができることになる。

【００６９】指紋から指紋データｆを生成する具体例について、以下に説明する。

【００７０】まず、指紋データリーダ３４で光学的走査により指紋パターンを取り入れ、これにフィルタ処理を施してから二値化する。さらに、二値化パターンを骨格化してマイニーシャを検出する。このとき、特徴点周辺の隆起線の形状を計測して、その結果から類似特徴点を排除する。最終的に抽出された特異点について、ある特徴点（親特徴点）の周囲で４個の子特徴点を選び、親特徴点の位置（ｘ、ｙ）、方向（ｄ）、子特徴点との関係（Ｒ１，Ｒ２，Ｒ３，Ｒ４）によって指紋の特徴データを生成する。すなわち、この場合の一指の特徴データは（x^i、y^i、d^i、$R1^i$，$R2^i$，$R3^i$，$R4^i$）(i=1, 2,…,N)のセットとなり、指紋データｆはこれらを組み合わせて羅列するなどによって生成することができる。

【００７１】このセットの数は、少なくとも同一人の同一指と判断できる程度の数が必要となる。また、リレーションＲは、皮膚の変形を考慮して特徴点間の隆線の数を用いることで不変な量とする。

【００７２】指紋データｆを生成した後、ICカード生成装置のハードディスク２６にインストールした暗号ソフトは、１組の非対称鍵を生成する（ステップＳ１０５）。すなわち、ここで、第１の非対称鍵である公開鍵Ｐと、第２の非対称鍵である秘密鍵Ｓが生成される。なお、非対称鍵の生成方法としては、べき乗除余タイプ暗号であるRSA方式を用いる。RSA方式は、最も代表的な非対称鍵方式であり、大きな整数の因数分解の困難さを利用したことを特徴とする。

【００７３】なお、この実施形態においては非対称鍵にRSA方式を採用しているが、RSA方式は、鍵によるデータ処理が一方向となっており、暗号化、復号化の方向がない。このため、RSA方式では、公開鍵で暗号化し、さらに秘密鍵で暗号化することは元のデータに戻すことと同じになってしまう。ただし、公開鍵（秘密鍵だけでも可）だけで、複数回の暗号化処理を行うことはできる。

【００７４】つぎに、利用者は、自己のパスワードWを

キーボード２８を介して入力する。ICカード作成装置は、このパスワードWをメモリ２２に読み込む（ステップS１０７）。

【００７５】ハードディスク２６に記録した暗号ソフトは、このパスワードWを種データとして共通鍵Wcを生成する処理を行う（ステップS１０９）。なお、ここで生成する共通鍵Wcは、パスワードWによって一義的に定まるものとする。

【００７６】さらに、暗号ソフトは、この共通鍵Wcによって秘密鍵S（ステップS１０５において生成済）を暗号化処理する。これにより、パスワードWに基づいて生成した共通鍵Wcによって暗号化したデータWc[S]が生成される（ステップS１１１）。なお、ここで用いるパスワードは、利用者が予め設定しておいたものを用いる。

【００７７】また、共通鍵Wcの生成方式としては、代表的なブロック暗号タイプであるDES方式を用いる。ブロック暗号とは、平分をブロック化し、ブロックごとに暗号変換を施すタイプの暗号であり、例えば、換字法（文字を他の文字で置き換える方法）、転字法（文字の順序を入れ換える方法）などが存在するが、ここでは、これらを組み合わせたものが用いられる。

【００７８】つぎに、暗号ソフトは、公開鍵P（ステップS１０５において生成済）を用いて、指紋データｆを暗号化し、公開鍵によって暗号化したデータP[f]を生成する（ステップS１１３）。このデータP[f]を、さらに公開鍵Pによって暗号化処理し、P[P[f]]を生成する（ステップS１１５）。

【００７９】このように、指紋データfを公開鍵Pを用いて二重に暗号化することによってデータP[P[f]]が生成される。なお、このデータP[P[f]]が、データ記録媒体に記録される第１の暗号化生体データである。

【００８０】ICカードライタ３１は、挿入されたICカード３２に、前述した公開鍵Pによって２重暗号化したデータP[P[f]]（ステップS１１５において生成済）に加えて、公開鍵P（ステップS１０５において生成済）および共通鍵Cによって暗号化したデータW[S]（ステップS１１１において生成済）を記録する。

【００８１】以上の処理によって、ICカードは作成される。このICカードは、システム管理者によって利用者に対して配布される。例えば、この発明を銀行のATMにおけるキャッシュカードを用いた現金の取り扱いに用いた場合は、銀行がICカード３２を上記のようにして作成し、利用者に対して配布する。

【００８２】利用者は、以下に説明するように、ユーザ認証時にこのICカード３２を用いることとなる。

【００８３】［利用者の認証手順］以下に、図７及び図４を用いて、上記のように作成したICカード３２を用いた認証の手続について説明する。なお、図７は、利用者の認証手順を示したフローチャートである。

【００８４】まず、ユーザ認証を受けようとする利用者は、クライアントＰＣ５の指紋データリーダ３４に指を触れる。これによって、指紋データリーダ３４は、指紋の読み込みを開始する（ステップS２０１）。さらに、クライアントＰＣ５の指紋データリーダ３４は、指紋の特徴を抽出して、指紋データｆ’を生成する（ステップS２０３）。ここでは、前述したICカード作成時における指紋データの作成方法において説明したのと同様のデジタルデータ生成処理（図６のステップＳ１０３における処理）が行われる。

【００８５】その一方で、利用者は、図４に示すクライアントＰＣ５のICカードリーダ３０に自己のICカード３２を挿入する。これにより、ICカードリーダ３０は、ICカード３２に記録された公開鍵データPを読み出す（ステップS２０５）。さらに、照合ソフトは、この公開鍵データPを用いて、ステップS２０３で生成した指紋データｆ’を暗号化処理し、データP[ｆ’]を生成する（ステップS２０７）。なお、このデータP[ｆ’]が、後に比較照合される一方の照合データ（第二の暗号化生体データ）であり、メモリ２２に記録される。なお、ICカードリーダ３０は、同時にICカード３２が備えるホログラムから電子透かしデータを読み取り、ICカード３２の真贋を判断する。

【００８６】つぎに、利用者は、キーボード／マウス２８を介してクライアントＰＣ５にパスワードWを入力する。これにより、クライアントＰＣ５は、パスワードWのデータを取得する（ステップS２０９）。なお、ここで入力するパスワードは、当然に前述のICカード作成時において（図５のステップS１０７）入力したパスワードと同じものを用いる。このパスワードWを用いて、ステップS１０９における処理（図５参照）と同様にDES方式により共通鍵Ｗｃが生成される。

【００８７】また、クライアントＰＣ５のICカードリーダ３０は、ICカード３２に記録されたデータWc[S]を読み出す（ステップS２１１）。さらに、照合ソフトは、この共通鍵Wcを用いて、ICカード３２から読み出したデータWc[S]を復号化し、元の秘密鍵Sの状態にもどす（ステップS２１３）。

【００８８】つぎに、クライアントＰＣ５のICカードリーダ３０は、ICカード３２に記録されたデータP[P[f]]を読み出す（ステップS２１５）。なお、データP[P[f]]は、公開鍵Pによって指紋データｆを２重に暗号化したものである。

【００８９】さらに、照合ソフトは、この復号化した秘密鍵Sを用いて、ICカード３２から読み出したデータP[P[f]]を復号化処理し、一重に暗号化したデータP[f]の状態に戻す（ステップS２１７）。この一重暗号化したデータP[f]が、照合ソフトに比較照合されるもう一方の照合データ（第３の暗号化生体データ）である。

【００９０】照合ソフトは、メモリ２２に記録された第２の暗号化生体データP[ｆ’]（ステップS２０７にお

いて、指紋データリーダ３４によって読み出した指紋データを暗号化処理したもの）と第３の暗号化データP[f]（ICカードリーダ３０によってICカード３２から読み出したデータP[P[f]]をステップＳ２１７において復号化処理したもの）とを比較照合することによって両データの同一性を判断し、以下のようなユーザ認証処理を行う（ステップS２１９）。

【００９１】比較照合の結果、両データが同一と照合手段が判断した場合は、正当な利用者として認証され、クライアントＰＣ５におけるセキュリティー保護状態が解除される（ステップS２２１）。これにより、その後、クライアントＰＣ５とサーバ１との間で通信が行うことができ、サーバ１とのアクセス実行も可能となる。

【００９２】これに対し、両データが同一でないと照合ソフトが判断した場合には、正当な利用者として認証されず、クライアントＰＣ５におけるセキュリティー保護状態が解除されない（ステップS２２３）。すなわち、かかる場合は、悪意の第三者による成りすましである可能性が高いため、クライアントＰＣ５とサーバ１との間ではアクセス実行が不可能となる。なお、このような場合は、クライアントＰＣ５よりサーバ１に対して警告を行うことによりセキュリティー管理者に注意を促すことがが望ましい。

【００９３】[その他の実施形態]なお、この実施形態においては、ICカード３２に記録する第１の暗号化生体データを生成するために、指紋データｆを非対称鍵の１つである公開鍵Ｐによって二重暗号化処理することとしたが、共通鍵によって指紋データを二重暗号化することによって、第１の暗号化生体データを生成してこの発明を実施してもよい。

【００９４】なお、この実施形態においては、ICカード３２から読み出した第１の暗号化生体データを非対称鍵によって復号化した後、第２の暗号化生体データと比較照合することとした。しかし、第１の暗号化生体データを復号化せずに、そのまま第３の暗号化生体データとして、第２の暗号化生体データと比較照合するようにしてもよい。

【００９５】例えば、この実施形態において、ICカード３２には、第１の暗号化生体データとして公開鍵Ｐにより二重暗号化したデータP[P[f]]が記録されており、このデータがそのまま第３の暗号化生体データとして第２の暗号化生体データP[P[f]]と比較照合されるような場合が該当する。この場合、第２の暗号化生体データは、利用時に取得した指紋データf'を公開鍵Pにより二重暗号化して生成する。

【００９６】また、上記のように第２および第３の暗号化生体データの比較照合は、一重暗号化した状態で行う場合に限られず、二重暗号化した状態またはそれ以上の複数回暗号化した状態で比較照合を行うようにしても良い。

【００９７】なお、この実施形態においては、生体情報に指紋の情報を用いたが、その他の個人の属性情報である声紋、筆跡、網膜の眼紋などの情報を用いても良い。

【００９８】なお、この実施形態においては、非対称鍵の生成方法としてRSA方式を用いたが、DSA方式などのその他の非対称鍵の生成方法を用いてもよい。また、共通鍵生成方式として、ブロック暗号タイプであるDES方式を用いたが、ストリーム暗号タイプを用いてもよい。

【００９９】なお、この実施形態においては、第１の非対称鍵として公開鍵Ｐを、第２の非対称鍵として秘密鍵Ｓを用いたが、これに限定されず、第１の非対称鍵として秘密鍵Ｓを、第２の非対称鍵として公開鍵Ｐを用いてもよい。

【０１００】なお、この実施形態においては、マイニューシャの特徴に基づいて指紋データｆを生成したがこれに限定されるものではなく、隆線の形状を単にビットマップデータに変換することで指紋データｆを生成するようにしても良い。

【０１０１】なお、この実施形態においては、共通鍵Ｗｃを生成するために利用者が予め設定したパスワードＷを用いたが、指紋情報などの個人の属性情報などをパスワードとして用いてもよい。

【０１０２】なお、この実施形態においては、データ記録媒体にICカード３２を用いたが、磁気カード、USBキーなどを用いても良い。

【０１０３】なお、この実施形態においては、本発明をクライアントＰＣ５のセキュリティー状態を解除するための認証に用いたが、これに限定されず企業におけるコンピュータ室の入退管理、銀行のATMにおける口座の取り扱いなどにも用いることができる。

【０１０４】なお、この実施形態においてはサーバ１が存在することとしたが、サーバ１が存在しないような場合であってもよい。例えば、クライアントＰＣ５のみが、ネットワーク３に接続されているような場合である。さらに、クライアントＰＣ５のみにおける認証についても、この発明を用いることができる。

【図面の簡単な説明】

【図１】この発明の概要図である。

【図２】この発明の実施形態の概要図である。

【図３】この発明を実施するためのシステム構成を示す図である。

【図４】クライアントＰＣの構成を示す図である。

【図５】ICカード生成装置の構成を示す図である。

【図６】データ記録媒体へデータを記録するまでの手順を示すフローチャートである。

【図７】利用者の認証手順を示すフローチャートである。

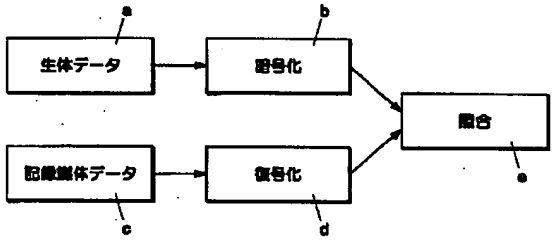
【符号の説明】

１・・・・サーバ

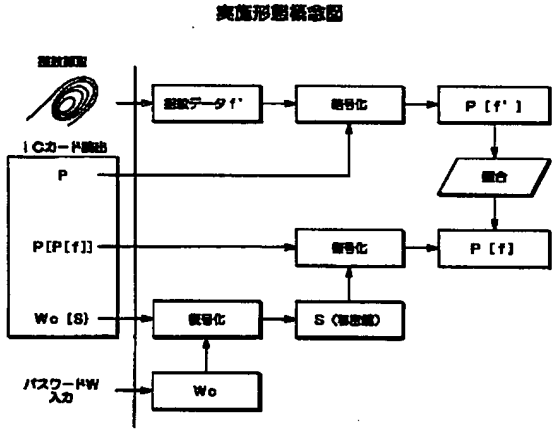
３・・・・ネットワーク

５・・・・クライアントＰＣ
２０・・・CPU
２２・・・メモリ
２４・・・ディスプレイ
２６・・・ハードディスク
２８・・・キーボード／マウス
３０・・・ICカードリーダ
３１・・・ICカードライタ
３２・・・ICカード
３４・・・指紋データリーダ

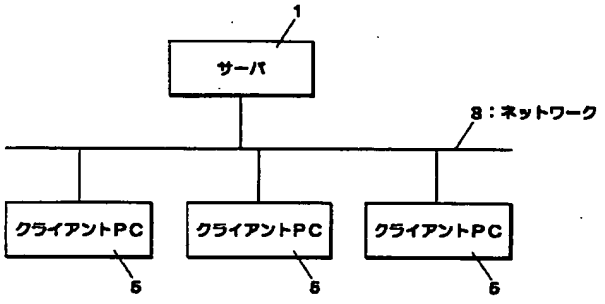
【図１】



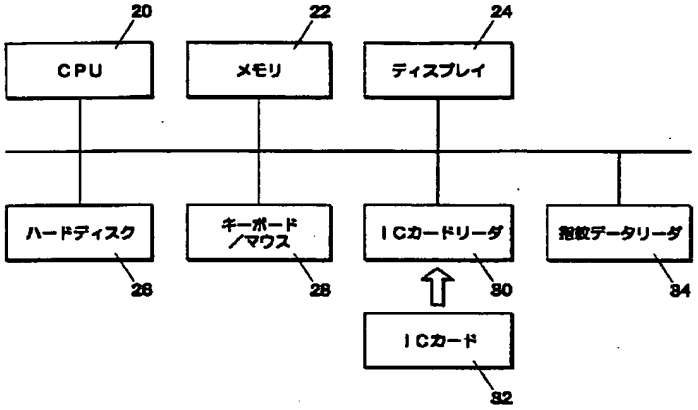
【図２】



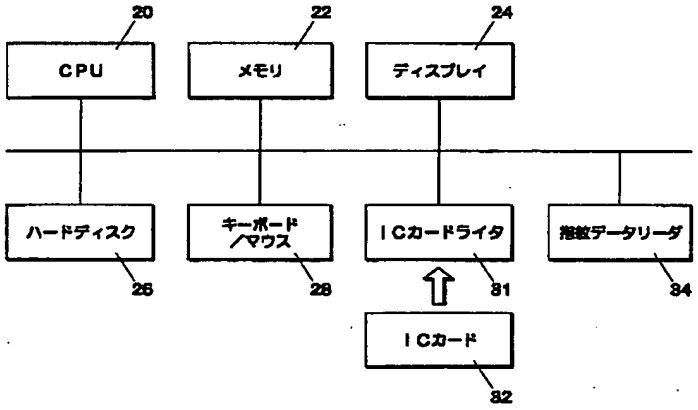
【図３】



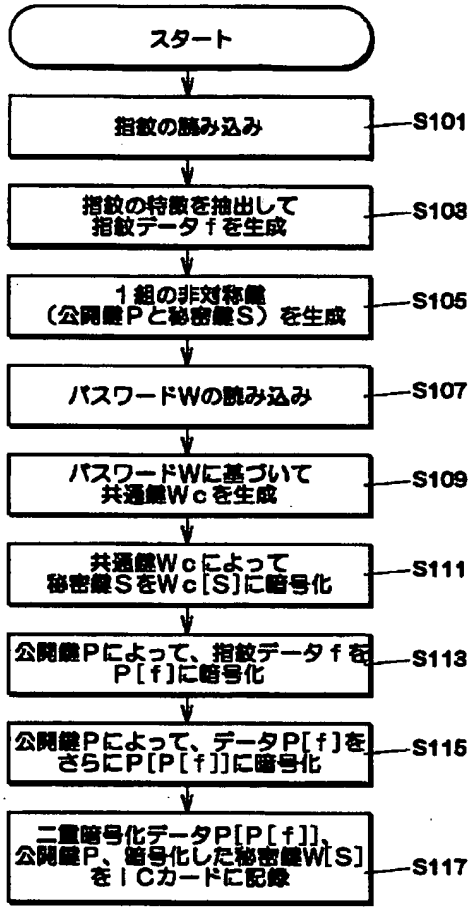
【図４】


20
22
24
CPU
メモリ
ディスプレイ
ハードディスク
キーボード
／マウス
ＩＣカードリーダ
磁気データリーダ
26
28
30
34
ＩＣカード
32

【図５】

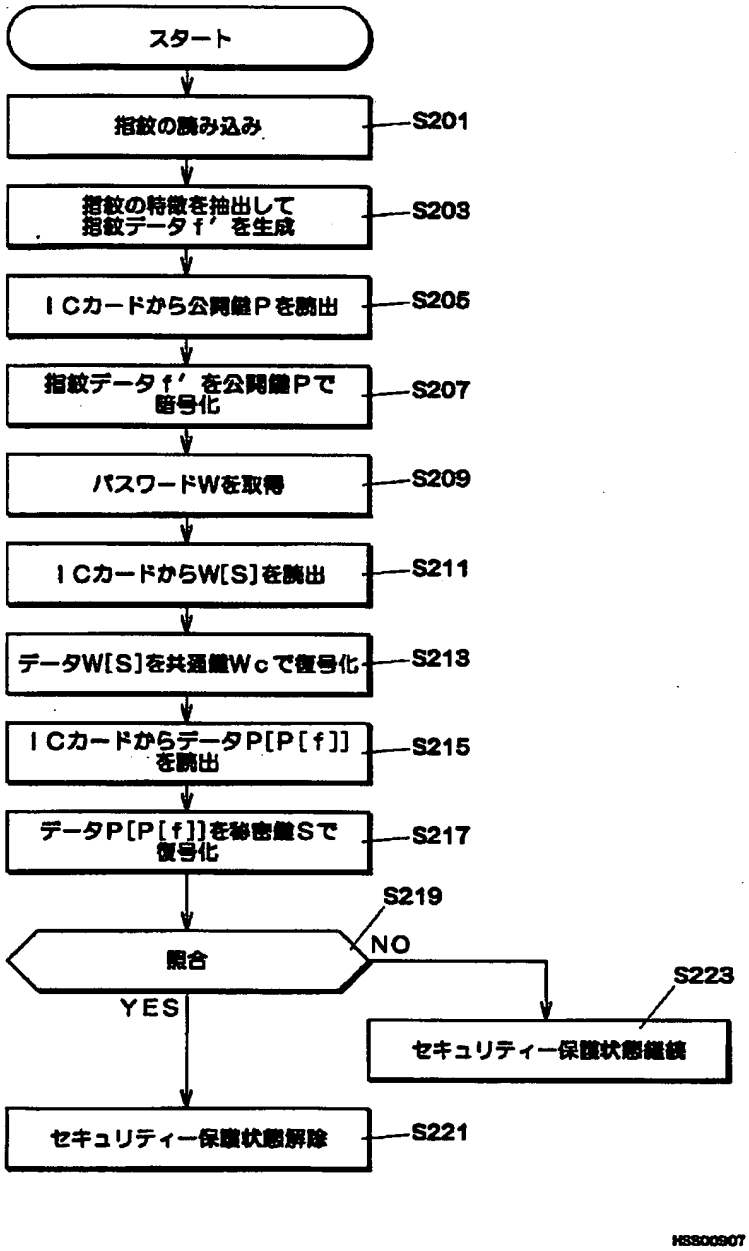

20
22
24
CPU
メモリ
ディスプレイ
ハードディスク
キーボード
／マウス
ＩＣカードライタ
磁気データリーダ
26
28
31
34
ＩＣカード
32

【図６】


スタート
指紋の読み込み
S101
指紋の特徴を抽出して
指紋データｆを生成
S103
１組の非対称鍵
（公開鍵Ｐと秘密鍵Ｓ）を生成
S105
パスワードWの読み込み
S107
パスワードWに基づいて
共通鍵Ｗｃを生成
S109
共通鍵Ｗｃによって
秘密鍵ＳをＷｃ[S]に暗号化
S111
公開鍵Ｐによって、指紋データｆを
Ｐ[ｆ]に暗号化
S113
公開鍵Ｐによって、データＰ[ｆ]を
さらにＰ[Ｐ[ｆ]]に暗号化
S115
二重暗号化データＰ[Ｐ[ｆ]]、
公開鍵Ｐ、暗号化した秘密鍵Ｗ[S]
をＩＣカードに記録
S117

H9300908

【図７】



フロントページの続き

(51)Int.Cl.[7]	識別記号	ＦＩ	テーマコード(参考)
		Ｈ０４Ｌ　9/00	６７３Ｅ

(72)発明者　植野　圭二
大阪府大阪市中央区内本町２丁目４番16号
株式会社日立システムアンドサービス内

Ｆターム(参考)　5B085 AE09 AE25 AE29
5J104 AA07 AA14 AA16 EA06 EA18
KA01 KA05 KA16 KA17 NA02
NA05 NA35 NA37 NA38